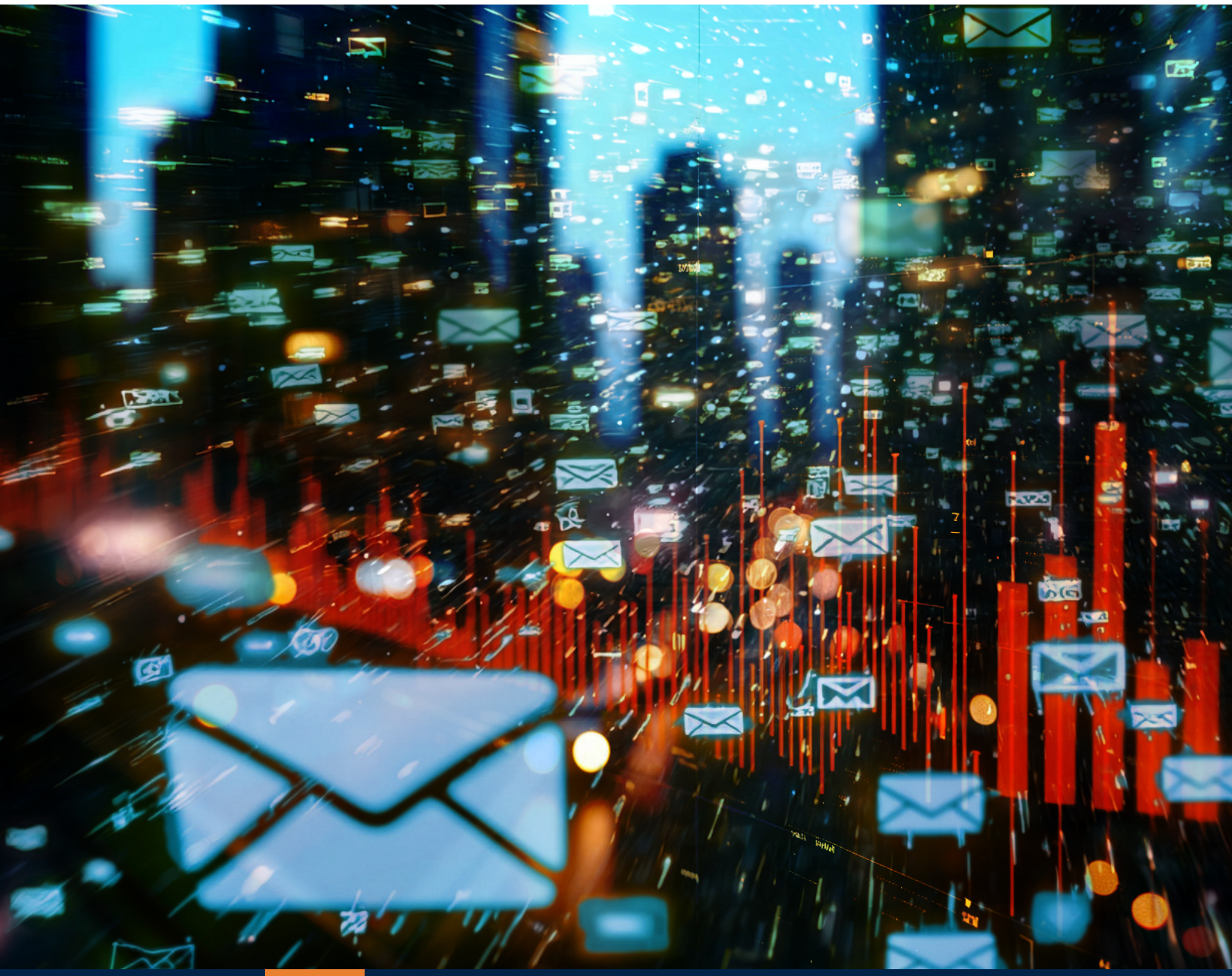
KnowBe4

The 3 Biggest Email Security Challenges Facing Financial Service Organizations



WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

0725US

INTRODUCTION

Financial institutions are under constant pressure to move fast, stay compliant and protect sensitive client data, all without letting anything fall through the cracks. And yet, one of the most commonly used tools in the business—email—remains one of the biggest sources of risk.

Despite advances in email filtering and encryption, the leading cause of email-related security incidents isn't a lack of tech—it's human error. In fact, **up to 68% of data breaches in financial services can be traced back to people making mistakes:** misdirecting sensitive documents, clicking the wrong link or failing to recognize a cleverly disguised phishing email.

Worse, **90% of outbound email security incidents go undetected,** according to KnowBe4 research, silently bypassing legacy systems. At the same time, third-party involvement in breaches has doubled, expanding the attack surface and regulatory exposure. With evolving compliance mandates and growing scrutiny around insider threats, financial institutions face a perfect storm of email risk.

Client trust is on the line, and one accidental disclosure could be all it takes to lose it.

Unfortunately, legacy tools and static policies can't keep up with the complexity and speed of modern communication. That's where Human Risk Management (HRM) platforms come in.

Read on to explore the biggest email cybersecurity challenges facing today's financial services organizations. From misdirected emails to insider threats and regulatory gaps, we'll break down what's really happening, and more importantly, how you can get ahead of it before mistakes turn into fines, breaches or lost clients.

CHALLENGE #1

Regulatory Compliance and Data Governance: Why Traditional Controls Aren't Cutting It

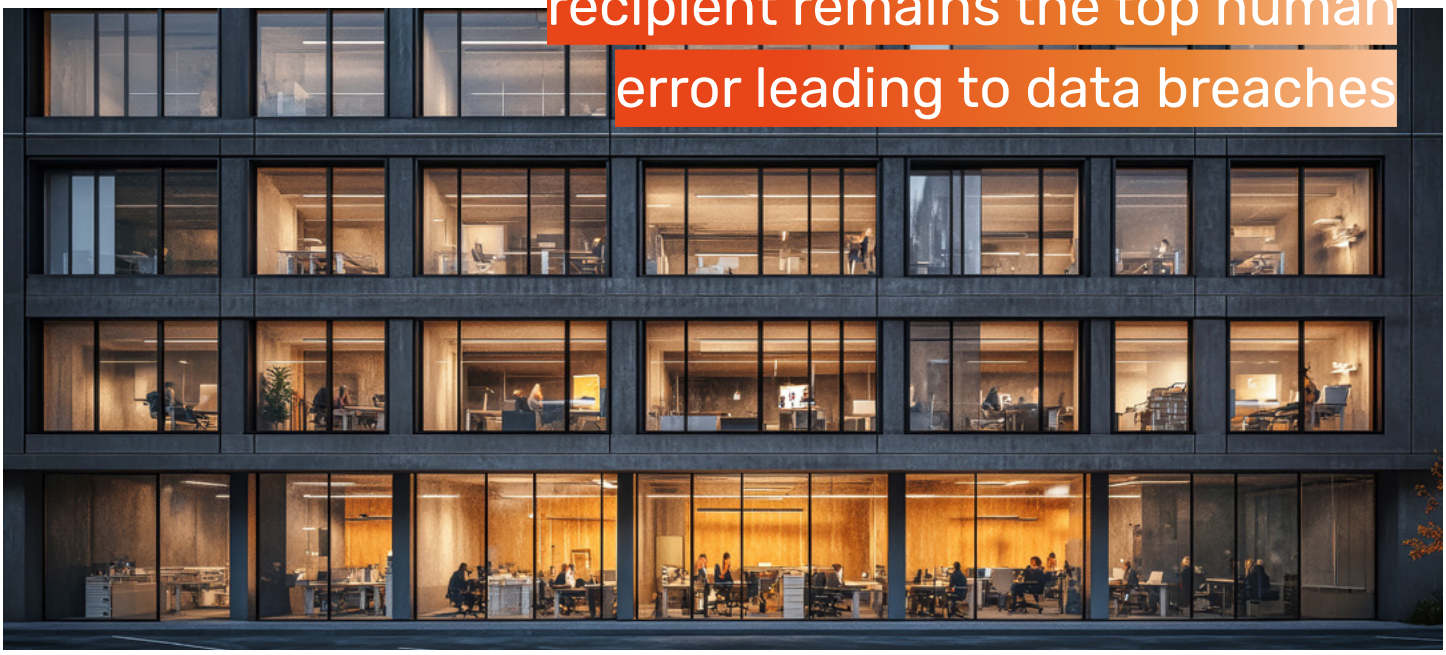
Financial institutions operate under some of the strictest data protection and privacy regulations in the world. These organizations handle highly sensitive client data and are foundational to global economic stability. But staying on the right side of GLBA, SEC, FINRA, GDPR and a growing list of international frameworks has become a complex, high-stakes balancing act.

The challenge? Most of today's compliance strategies are still too focused on systems and not enough on people. That's a problem when 68% of data breaches are caused by human error, not infrastructure failures.

Let's take "misdelivery" as an example—sending client financials to the wrong recipient. It sounds simple, but it remains the top human error leading to breaches. And regulators are taking note. In fact, FINRA reported a 63% increase in fines in 2023, with penalties totaling $89 million. That number is only expected to grow as scrutiny tightens.

Meanwhile, many organizations are still relying on static data loss prevention (DLP) rules and legacy compliance checklists that were built for slower, simpler workflows. These tools often miss the nuanced, real-world behaviors that create regulatory risk, such as a distracted adviser emailing a spreadsheet to the wrong "John Smith."

Sending client financials to the wrong recipient remains the top human error leading to data breaches



A Smarter Approach: HRM

HRM platforms offer a proactive path forward. Instead of just detecting issues after the fact, they work in real time to prevent violations before they occur.

Here's how:

- **Behavioral analysis** flags risky user actions, such as sending confidential client data to personal or unusual addresses
- **Context-aware scanning** identifies sensitive financial data in emails and attachments, alerting users to potential disclosure before they hit send
- **Recipient anomaly detection** learns typical communication patterns and warns when something seems off, such asa CFO sending payroll files to an unfamiliar Gmail address
- **Real-time policy enforcement** blocks risky messages or prompts users for confirmation, helping prevent mistakes without slowing down workflows
- **Audit-ready reporting** documents every action, giving compliance teams and regulators the evidence they need to show the organization was actively mitigating risk

Regulatory compliance and data governance aren't just about avoiding penalties—they're about earning trust. And in a business where trust is everything, you can't afford to leave human risk unmanaged.

The Benefits

By shifting from reactive to proactive compliance strategies, financial institutions can:

Uncover 10x more data breach risks that traditional tools miss

Avoid costly fines by demonstrating real-time enforcement, not just static policy documentation

Streamline regulatory reporting with incident prevention metrics that are accurate, automated and aligned with what auditors expect

Protect client trust and institutional reputation by preventing the kinds of data incidents that make headlines—and drive customers away

CHALLENGE #2

Client Data Protection and Trust: Balancing Speed with Security in High-Stakes Relationships

In wealth management and private banking, client trust is everything. Relationships are built over years and are grounded in the belief that their financial adviser, firm or institution can be trusted to act quickly, accurately and securely.

But in today's digital-first world, that trust is under pressure from both sides. Clients expect fast, seamless service, often in response to time-sensitive financial requests. At the same time, regulators and cybercriminals alike are watching every move, and the risks of accidental data exposure have never been higher.

Here's the reality: legacy systems and manual approval processes often slow things down. Advisers trying to move quickly to meet client needs may bypass internal protocols or unintentionally misdirect sensitive data, such as transaction details, portfolio statements or private wealth management strategies. All it takes is one wrong email address or unauthorized file share to trigger a serious breach.

And when that happens? **One in three clients say they'd switch providers** after a data incident.
In a hyper-competitive market, it's both a loss and a reputational impact that ripples across your organization.

How HRM Protects Clients—and Relationships

HRM platforms are built to prevent data leaks before they happen, without getting in the way of fast, responsive service.

They continuously monitor for risky behavior, such as attaching sensitive client files to emails or replying to suspicious domains. Data handling policies are enforced automatically, not manually, so advisors don't have to jump through hoops just to do their jobs. And when something doesn't look right—say, a file going to a previously unknown recipient—the platform prompts the sender with a smart, just-in-time warning.

It's like having a real-time safety net that doesn't slow you down.

What makes this approach so effective is that it works in the background. Clients get the rapid service they expect. Advisors aren't bogged down by outdated processes. And security and compliance teams can rest easier knowing that proactive safeguards are doing their job—even when no one's looking.

In today's market, trust isn't just earned through performance—it's reinforced through every secure interaction. With the right email security and HRM tools in place, financial institutions can confidently protect both their data and their most valuable relationships.

Key Benefits That Build Competitive Advantage

Adopting a smarter approach to client data protection delivers a powerful mix of outcomes:

Maintain rapid client response times without compromising on data security

Eliminate workflow bottlenecks that frustrate advisers and delay important transactions

Enhance client retention by protecting sensitive data behind the scenes before issues arise

Build a competitive edge by showing clients and regulators that you can be both secure and responsive

CHALLENGE #3

Insider Risk and Information Barriers: Why Static Controls Can't Keep Up

Insider threats in financial services aren't just about malicious actors. Often well-meaning employees operating in complex environments without clear boundaries are the cause. And in a world where teams rely on real-time communication tools like chat, video and email—often across hybrid or distributed workforces—the challenge of managing insider risk is only getting harder.

Financial institutions are under strict obligations to maintain information barriers, or "ethical walls," between business units that could have conflicting interests. Think trading desks and research analysts, or investment banking and wealth management teams. These walls are critical for avoiding insider trading, market manipulation and other forms of misconduct. Regulators like the SEC don't just recommend these controls—they require them. And when things go wrong, **penalties reach tens of millions of dollars per violation**.

The problem? Traditional rules-based DLP tools aren't designed for this kind of dynamic environment. Static policies may block obvious red flags, but they struggle to detect nuanced risks across fast-moving, informal communication channels. And they often overcorrect—blocking legitimate collaboration and slowing down teams trying to get work done.

Data loss prevention tools aren't designed for the dynamic environments of financial service organizations

A Smarter Approach: Adaptive Controls Through HRM

HRM platforms take a fundamentally different approach to insider risk. Rather than relying on rigid, one-size-fits-all rules, HRM platforms leverage AI-powered behavioral analytics to understand how users communicate, detect anomalies and enforce adaptive controls in real time.

For example, if an employee on the trading desk suddenly starts communicating with someone on the research team in a way that deviates from normal patterns, the system flags it. If sensitive information is being shared that shouldn't be, it's automatically blocked or escalated—before it becomes a compliance issue.

These platforms learn communication norms within your organization and use that intelligence to enforce dynamic information barriers. That means fewer false positives, more effective protection and no need to slow down legitimate business operations. And when something does require investigation, compliance teams get detailed alerts with full context, making it easier to act quickly and decisively.

In today's interconnected, high-velocity work environment, protecting against insider threats isn't just about controlling access, it's about understanding behavior. With the right HRM tools, financial institutions can maintain regulatory compliance, protect sensitive information and empower employees to work securely and efficiently across the business.

Key Benefits That Go Beyond Compliance

Implementing adaptive, behavior-driven insider risk controls brings significant advantages:

Reduce insider risk exposure with intelligent, real-time enforcement that adapts to your environment

Prevent violations before they escalate, avoiding costly fines, regulatory scrutiny and reputational damage

Enable compliant collaboration between departments by using smart boundaries, not blunt-force rules

Deliver audit-ready evidence to regulators that proves your institution is actively monitoring and enforcing ethical walls

Conclusion

Financial institutions are expected to move fast, stay compliant and secure sensitive data—all at the same time. But when human error is the root cause of most breaches, legacy tools that focus only on infrastructure fall short. HRM platforms offer a smarter approach: one that proactively prevents mistakes, automates security and delivers real transparency.

By addressing regulatory compliance, preserving client trust, and managing insider risk before problems arise, financial organizations can reduce violations, stay agile and protect what matters most. The result? Fewer breaches, fewer fines and a stronger, more resilient institution built for today's challenges.

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk.

KnowBe4 offers a comprehensive AI-driven "best-ofsuite" platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats. The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents, and more.

As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization's biggest asset.

For more information, please visit **www.KnowBe4.com**

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com